Continuous Threat Exposure Management (CTEM)

Service Description

TABLE OF CONTENTS

1 Continuous Threat Exposure Management

1.1 Document Objective

This document (“Service Description”) describes the service features, components, and terms of the Continuous Threat Exposure Management (CTEM) (“VMaaS” or “Services”) that UVC will provide to the designated customer listed in a contractual binding Statement of Work (SOW). The specific quantity and type of the Services purchased by Client will be documented in a SOW between the parties.

1.2 Service Overview

The Continuous Threat Exposure Management service provides delivery vulnerability assessments of Client’s environment. The Service consists of automated and recurring vulnerability and compliance scanning. continuous analysis and assessments of Client’s assets.

1.3 CTEM Service Tiers

UVC offers Continuous Threat Exposure Management in delivery model coupling both system generated attack simulations as well as human modeled tradecraft. UVC delivers vulnerability scanning, remediation tracking workflow, reporting, and trending of a Client’s environment. IP level is based on Client’s technical scanning requirements.

The offering includes the following:

- **Platinum** – The Platinum option provides unlimited scanning recurrence of Client’s internal, external, and cloud-based live IP addresses. Scans of external IPs are conducted remotely. Scans of internal and cloud-based IPs are conducted from one or more Scan Appliances placed on Client’s network or in Client’s leased virtual datacenter. Scan Appliance quantities are restricted to two (2) per Client. User accounts are limited to three (3) per Client. Additional appliances and user accounts are not available at the IP level or service level.

The features are described further in the chart below.

Service Feature	Platinum	Description
Initial Implementation Support	☑	Implementation team available remotely for implementation support
Extended Data Retention	☑	Data is stored remotely for contract term
Vulnerability Reporting	☑	Self-service vulnerability and compliance reporting within the capabilities offered in the Tenable tool

Enterprise Security portal	☑	Vulnerability data available through the Enterprise Security portal
Scan Scheduling	☑	UVC will schedule and manage recurring scans
Quarterly Scan Review	☑	UVC will review scan results with Client each quarter, upon Client request
Profile Setup	☑	UVC will adjust scan profiles based on Client criteria
Group/Asset Value/Asset Owner Entry	☑	UVC will import Client-created group, asset, and owner data.
Asset Compliance Policy Entry	☑	UVC will enter an asset configuration policy within the compliance technology.
On-Demand Scan Request	☑	UVC will schedule Client scans on request with three (3) business days advance notice

UVC will work with the Customer to advice on the appropriate Tier of service for their specific environment consideration of the following:

- Live IP address quantity
- Application quantity
- Internal and/or external scanning
- Scanning appliance quantity
- User account quantity
- Scanning recurrence

2 Customer and UVC Responsibilities

The following responsibility assignment describes the participation required by both Customer and UVC in completing tasks or deliverables for a project or business process to facilitate successful service delivery. The key components of the services described are summarized and elaborated upon as follows:

1. **Service Transition - Planning and Support**
2. **Service Transition – Managed Component Activation**
3. **Customer Success Advisory and Reporting**

2.1 Service Transition – Planning and Support

Summary: UVC and Client will work together to provide details on the scope of the Services, and to define plan for establishing connectivity between UVC and the Vulnerability Management platform.

UVC Responsibilities	**Client Responsibilities**
▪ Define the high-level scope of work required to transition the in-scope Vulnerability Management, including all items detailed below ▪ Identify a single point of contact (SPOC) to engage with Client during the Service Transition ▪ Perform any other tasks designated as UVC's responsibility in the Transition Plan by the date specified in the Transition Plan	▪ Unless as otherwise agreed in writing, provide the reasonably requested inventory and topology information by the dates provided in the Transition Plan ▪ Review and approve Transition Plan, including Activation date(s) ▪ Identify a SPOC to engage with UVC throughout the Service Transition period ▪ Perform tasks specified as Client's responsibility in the Transition Plan (outlined below) by the date specified in the Transition Plan

Output: Transition Plan

2.1.1 Provisioning, Activation, and Service Commencement Provisioning

Provisioning refers to the service setup activities. The Standard Provisioning period begins at receipt of the signed SO by MSS Deployment Team and ends with the commencement of the service. The provisioning and setup period is dependent on a number of factors, such as the number of devices (if applicable), the number of physical sites, the complexity of the network and Client requirements, and the ability of Client to provide UVC with requested information within a mutually agreed-upon timeframe. UVC does not provide SLAs for completing Device service setup within a specified period of time.

2.1.2 Provisioning into Client On-Premises Networks

Standard Provisioning activities include:

- Scheduling Kick-off and Solution Design call (assumes receipt of SO by MSS Deployment Team)
- Information Gathering (UVC provides information requirements and forms for completion to Client)

- (Optional/as needed) UVC design of a solution architecture diagram (assumes UVC receipt from Client of complete and accurate information and diagrams)
- Configuring Client Relation Management ("CRM") / Ticket system (assumes Client approval of MSS solution design diagram(s))
- Configuring the appliance (if applicable)
- Shipping the appliance – ground shipping (if applicable) Provisioning into Client

2.1.3 VMS Service Activation Service

Activation and commencement consist of the following phases:

- Information Gathering
- Site Planning and Preparation
- Clients that require an internal scanning appliance

2.1.4 Information Gathering

Once UVC receives the Service Order, UVC provides Client with a Service Activation Profile (“SAP”) to be completed. SAPs include information required to provision the Service such as contact information, IP addresses, URLs, telephone numbers, and scan appliance locations.

2.1.5 Site Planning and Preparation

If scanning options are selected that include internal scanning, and for which Client requires use of a Scan Appliance, Client is responsible for ensuring that the implementation site complies with UVC’ physical/environmental requirements. Using data gathered during the Information Gathering phase, UVC determines the number of Scan Appliances required for the Service(s) and the appropriate deployment location(s) of the Scan Appliance(s) within Client’s environment. If changes to Client’s existing network architecture are required for Service implementation, UVC communicates these changes to Client.

2.2 Service Transition – Managed Component Activation

Summary: With Client’s assistance, UVC will connect the MAGE AS/DR platform Vulnerability Management components to the Client’s environment which may include implementation of necessary hardware or software components. UVC will perform tests to confirm that the Components meet technical readiness requirements and Activate the UVCVMS Components onto the MAGE Platform.

UVC Responsibilities	**Client Responsibilities**
▪ Provide notification to Client that Activation is complete. ▪ Provide a documentation to Client to describe necessary steps to configure the Vulnerability Management Components	▪ Configure access and implement requirements as described in the UVC documentation. ▪ Unless UVC is performing installation services, perform any required hardware or software installations, configuration changes and other stabilization activities required to enable connectivity and communication between the UVCVMS Components ▪ Assist UVC in establishing and validating bidirectional management connectivity between the UVCVMS Components ▪ If desired, review and monitor UVC's ready for use testing and results. ▪ Complete or assist in all functions outlined below
Output: N/A	

2.2.1 Service Commencement

The Service Commencement will occur on the date listed on the Service Activation Profile provided the following conditions have been met (as applicable):

- Information Gathering is complete
- Site planning and preparation is complete (if applicable)
- Client data is available on the portal (Vulnerability Scanning, Asset Compliance Scanning)

2.2.2 Change Control

Clients can reschedule the date and time of any additional services by contacting UVC, via the portal, email or telephone, at least five (5) business days prior to the next scheduled test or scan. A new date for the test or scan must be provided when Client contacts UVC to reschedule. All tests and scans must be completed within the applicable Service period.

Unused tests and scans will not be refunded and cannot be used after the applicable Service period has expired

2.2.3 Portal

UVC provides Client with access to Client Security portal (“portal”). The portal may only be accessed by the named individuals specified by Client during the Information Gathering phase. All information received by Client through the portal is solely for Client’s internal use and may not be re-distributed, resold, or otherwise transmitted outside of Client’s organization.

2.2.4 Client Requirements

UVC requires Client to agree to certain conditions of service delivery.

2.2.5 VMaaS Deliver

The following procedures apply to the delivery of UVCVMS:

- Total IP quantities selected are limited to unique live IP instances and may not be rotated throughout the term of the contract for Enterprise, Express, and Express Perimeter accounts.
- Scan results and suggested remediation guidance are made available on the Tenable portal in real time as the scan is completed.

2.2.6 Data Backups

The Client acknowledges and agrees that the scanning of IP addresses and/or domain names may expose vulnerabilities and, in some circumstances, could result in the disruption of Services or corruption or loss of data. The Client agrees that it is Client’s responsibility to perform regular backups of all data contained in or available through the devices connected to Client’s IP address and/or domain names.

2.2.7 Cloud-Based IP Address Acknowledgement

The Client acknowledges that the IP address of cloud-based assets is subject to change. The Client agrees that it is Client’s responsibility to identify the specific IP addresses of cloud-based assets that are to be scanned.

2.3 Customer Success Advisory and Reporting

Summary: UVC Incident Response will host a remote service review meeting on a regularly established cadence. The operational review will provide reports on current threat patterns, detection volumes, and trended events and similar relevant incident information.

UVC Responsibilities	Customer Responsibilities
▪ Provide recommendation on how to improve services, processes, and/or technologies based on data outputs from services and business intelligence tools ▪ Identify gaps between procured services and Customer goals. If applicable, highlight opportunities where other services can support Customer goals.	▪ Participate in established meeting cadence. ▪ Designate appropriate persons to review and approve (if desired) recommendations. ▪ Act on recommendations from UVC, including determining any dependencies resulting from the recommended actions.

Output: Reports

3 Services Terms

3.1 Scope of Additional Services

Unless the Services are expressly provided for above, all other UVC services are out of scope for this Service Description.

3.2 Vulnerability Reporting

UVC provides Client with full access to the Tenable portal to run a variety of reports. Executive Remediation Reports, High Severity Reports, Top 20 Reports, Patch Reports, and Scan Results are examples of vulnerability reports that are available via the Tenable portal. Report capabilities are restricted to the capabilities of the platform and are Client's responsibility to generate. Additional scan report result information is as follows:

- Vulnerability reporting with a description of each vulnerability, level of severity, business and technical impact, CVSS, remediation suggestions, and links to relevant sites Discovery reporting, detailing live hosts discovered on the network, including graphical maps
- Trending of vulnerability data
- Vulnerability remediation tracking and workflow

3.3 Tenable Portal

UVC provides Client with access to the Tenable portal through use of the SSO functionality. The Tenable portal may only be accessed by the named individuals specified by Client during the Information Gathering phase (defined below) and identified on the Service Activation Profile ("SAP") or by the individuals who have been added to the list of named individuals after Service Activation. All information received by Client through the Tenable portal is solely for Client's internal use and may not be re-distributed, resold, or otherwise transmitted outside of Client's organization. Within the Tenable portal, Client is able to access a dashboard, a network discovery map, perform discovery scans, schedule vulnerability scans, run reports, track remediation status, and perform asset searches.

3.4 Scan Scheduling

UVC will work with Client to gather targeted IP address and/or URL information and then schedule, run, and maintain scans. The Client must contact UVC with relevant scan information within ten (10) days of the date they wish to scan.

3.5 Quarterly Scan Review

The Client contacts UVC ten (10) days prior to the requested date to schedule a conference call to review scan findings, answer questions related to scan results, and discuss remediation strategies. The conference call is limited to one (1) hour each quarter.

3.6 Profile Setup

UVC will assist Client in selecting individual scan engine profiles as requested by Client.

3.7 Asset Compliance Policy Entry

UVC will enter a Client asset compliance policy into compliance technology. Policy entries are limited to three (3) per contract term and must be pre-defined by Client. Up to eight (8) policy, control, and value changes are allowed per month. UVC will not define asset policies or custom controls. This is the responsibility of Client. Client user defined controls will be evaluated on a case-by-case basis. The Client will be responsible for managing and entering exceptions.

3.8 On-Demand Scan Request

UVC will run on-demand scans at Client request. On-demand scans are limited to five (5) per month. Client-run on-demand scans are unlimited. UVC requires at least 3 business days of lead time to schedule and run the scan.

3.9 Asset Compliance

Asset Compliance assists organizations with increasing security by assessing compliance with policies in regard to system configurations and access controls. Through credential-based authentication, UVC collects operating system configurations and application access controls from hosts and servers within the enterprise and then maps this information to pre-defined policies in order to measure compliance with external regulations and internal security requirements.

3.10 Web Application Scanning

UVC will run on-demand scans against the Clients webservers. From OWASP Top 10 risks to vulnerable web app components, UVCVMS Web App Scanning provides comprehensive and accurate vulnerability scanning. UVCVMS delivers safe and automated vulnerability scanning to that can easily scale to cover the entire online portfolio, so security professionals can rapidly assess their web applications without heavy manual effort. Web Application Scanning provides high detection rates with minimal false positives, ensuring you understand the true cyber risks in your web applications

3.11 Container Scanning

UVC Container Scanning using Tenable.sc integrates into your DevOps pipeline to eliminate security blind spots without slowing down software development. UVC Container Scanning delivers end-to-end visibility of Docker container images, providing vulnerability assessment, malware detection and policy enforcement prior to and after deployment. Compatible with the DevOps toolchain your developers already use, Tenable.sc Container Security brings proactive visibility and security to solve the security challenges of containers at the speed of DevOps.Tenable.sc Container Security provides “at-a-glance” visibility into your container environment, including images, policies, repositories and key operational information.

3.12 IoT Scanning

At the heart of every industrial facility is a network of industrial control systems which is comprised of purpose-built controllers. Sometimes known as Programmable Logic Controllers (PLCs) and Remote Terminal Units (RTUs), these controllers are dedicated industrial devices that serve as the bedrock of all industrial processes. Today's sophisticated Operations Technology (OT) environments have a large attack surface with numerous attack vectors. Without complete visibility, security and control across the converged IT and OT, the likelihood of getting attacked is not a matter of 'if'; it's a matter of 'when'.

UVC IoT Scanning using Tenable.IO protects industrial networks from cyber threats, malicious insiders, and human error. From threat detection and mitigation to asset tracking, vulnerability management, and configuration control, our Industrial Control System (ICS) security capabilities maximize the safety and reliability of operational environments. The solution delivers situational awareness across all sites and their respective OT assets - from Windows Servers to PLC backplanes - in a single pane of glass.

3.13 UVC Recommendations

To the extent that Client fails to implement any reasonable UVC recommendations or requirements with respect to the VMaaS Components or the Services, UVC shall have no responsibility for any delays or failure(s) regarding the performance of the Services or its impact to the Client.

3.14 Services Management and Governance

Client, not UVC, is responsible for coordinating any complementary services. If Partner wishes to directly receive Client data (e.g. Security Incident tickets) and/or perform responsibilities or complementary services on Client's behalf, Partner will obtain written permission from Client and if requested, provide UVC with a Letter of Authorization from Client, allowing this sharing of data and coordination of Services.

UVC and Client (and if requested and agreed, Partner) will implement a governance function with the following goals: discuss alignment of the services to Client's business needs, identify opportunities to improve the Services (e.g., increase quality or reliability), and similar matters. The parties will conduct periodic governance meetings as mutually agreed. Both UVC and Client will make available appropriate members of its IT, business, and leadership organization for the governance meetings, as applicable.

4 Legal Terms

4.1 Order of Preference

This Service Description is subject to the applicable reseller agreement between the parties (“Agreement”). If there is a conflict between this Service Description, an Ordering Document, the applicable Agreement, or any Supplement to this Service Description, the following priority will apply (from highest to lowest):

a) any Ordering Document, as applicable

b) any Supplement(s)

c) the Service Description

d) the applicable Agreement

4.2 Compliance with Laws

UVC will comply with applicable laws, rules and regulations, including, but not limited to, all applicable export control laws and regulations. Client will comply with all applicable laws, rules, and regulations related to the receipt and use of the Services and will obtain all approvals and licenses required by any third parties related to the RTaaS Components, Client’s locations, systems, software, and network as are reasonably necessary for UVC to provide the Services.

4.3 Sale via UVC Authorized Reseller

Partner is responsible for obtaining appropriate agreements with Client reflecting the applicable terms of this Service Description, including (without limitation) requiring the performance of Client responsibilities. If Client has purchased these Services through a UVC Authorized Reseller and were not provided a Service Description by the Partner, then this Service Description is incorporated into the agreement between the UVC Authorized Reseller and Client governing the Authorized Reseller’s provision of the Services to Client (if applicable, the “Agreement”).

4.4 License

Client receives a limited, non-transferable, non-sublicensable, internal use, license to use the executable version of Portal, and any software provided by UVC as part of the Services only to the extent and duration reasonably required to receive the Services. There are no warranties associated with these items outside of their use as part of the Services. Upon expiration or termination of the Services, the license to the Portal and any associated software will automatically terminate. Note, this license is separate from the licensing and rights associated with the RTaaS Components, which are licensed separately.

4.5 Security and Data Privacy Program

UVC, and Client will maintain a reasonable information security and data privacy program with appropriate technical, administrative, and physical safeguards designed to prevent any (i) unauthorized access, use, distribution, or deletion of Client’s data and (ii) compromise of the RTaaS Components or AS/DR. If UVC and Client do not have a mutual data protection agreement in place (or equivalent privacy and data protection terms), the following Mutual Data Protection Agreement is incorporated into this Service Description.

4.6 Confidential Information

The ticket information, including recommendations to resolve Security Incidents, Charges, Portal, and Service Level performance information are Confidential Information. This information may not be used for any purpose other than in connection with Client's use of the Services.

4.7 Telemetry Data

UVC may collect data on Client's usage of the Services in order to maintain, improve, market, or promote the Services. In addition, UVC may use anonymized and aggregated data on Client's use of the Services, Managed Component performance (UVC products only), and network performance ("Telemetry Data") to create or improve its products and services. UVC will comply at all times with applicable law related to UVC's collection and use of the data above and will use reasonable physical, technical, and procedural means to protect the Telemetry Data that contains Personal Data in accordance with the UVC Online Privacy Statement, which is made available at or such other site(s) as UVC may publicly communicate from time to time.

4.8 Subcontractors

UVC may use subcontractors to provide services to Client on its behalf for the purposes of providing the Services. UVC will remain responsible for its subcontractors' compliance with the obligations under this Service Description, any Supplement, and the applicable agreement between UVC and Client. References to UVC in this Service Description and any Supplement shall include its subcontractors, as applicable.

5 Service Levels

The Service Levels (“Service Level”, “SLA”, “SLO”). describes the parties’ responsibilities and sets UVC’s performance targets for the VMaaS Services. The SLA only applies to the Penetration Testing and Red Teaming as a Service (VMaaS Services). UVC will categorize and respond to findings according to the Priority level methodology described in Section 3 Service Terms. Subject to the terms of this SLA, UVC will perform the VMaaS Services so that they will meet or exceed the performance targets Service Levels.

For those Services Levels labelled as Service Level Objectives (SLO), they are objectives only. If UVC fails to meet the Service Levels below, it will review the reasons it failed meet the Services Levels and will use commercially reasonable efforts to remediate the cause of the failure.

5.1 Performance Measurement

UVC will use its standard processes and tools for measuring its performance and determining whether the Service Levels were achieved using Key Performance Indicators (KPIs). KPIs are performance indicators only and there are no financial or legal penalties if UVC does not achieve them. Performance will be managed as follows:

- The window to measure performance against the Service Levels is the Measurement Period. The first Measurement Period will begin 60 days after Service Activation.
- Within thirty (30) days of the end of each Measurement Period, UVC will provide to Client a report on the Service Level Performance for the relevant Measurement Period (“Performance Report”).
- Within 30 days of receiving the Performance Report (“Review Period”), Client should review the report and submit a written claim for Service Credits or dispute the report.
- If Client disputes the Performance Report, the parties will review the matter, including providing underlying information to support or dispute the contents of the Performance Report.
- The Performance Reports and any underlying data provided to Client to support the Performance Report is Confidential Information and may not be publicized.

5.2 Client Responsibilities

- Client will provide UVC with a single point of contact to cooperate with UVC and respond to any UVC requests to help verify Service Level Performance
- Client will provide such information and assistance that UVC reasonably requests to help UVC verify Service Level Performance.
- Client will comply with all of its responsibilities as described in the Service Description for RTaaS Services, including any referenced documents.

5.3 SLA Exceptions

Any failure by UVC to achieve the Service Levels will be excused if caused by:

a) A material act or omission by Client in breach of the terms and conditions of the Agreement, the Service Description, and/or the Ordering Document;

b) Client's failure to comply with its obligations or responsibilities under the Service Description or this SLA;

c) Any mutually agreed schedule of activities that causes service levels to fall outside of measured and defined Service Level obligations set forth in this SLA;

d) Any delays or faults caused by Client, third party equipment, software, services, support, or vendors not under the control of UVC (e.g., Carrier cycle time);

e) Periods of maintenance where updates, patches, etc. are installed and configured (i.e. Maintenance Windows);

f) A Force Majeure Event;

g) Any UVC or third-party hardware dispatch and replacement, which may be covered under a separate agreement;

h) The RTaaS Components being past the End of Support (EOS) date or not covered by support and maintenance.

i) Software defects that require installation of major software updates or reinstallation of the software on the UVC equipment

j) Changes in the RTaaS Components or network that were not validated or approved by UVC or delays by Client in implementing Changes requested by UVC or otherwise agreed between Client and UVC;

k) Failure to implement UVC's recommendations necessary to remediate Incidents; l) Failure by Client to provide a required response necessary for UVC to meet the Service Levels (Please note: Incident Tickets will be on "hold" for any period of time UVC is delayed in receiving required information from the Client, the End User, or applicable third-party service providers);

l) Any conditions existing prior to UVC management of the RTaaS Components, including any incident, problem, error or other event subject to an open support ticket from a legacy or other third-party service provider; and/or

m) Changes to the RTaaS Components that were not approved by UVC.

5.4 Security Audit

If there are repeated Security Incidents that UVC reasonably believes can be prevented through the proper use of the RTaaS Components and Services, UVC may conduct, at its own expense and discretion, a review of Client's security environment. Client will reasonably cooperate with this review. Following any such review, Client will make commercially reasonable efforts to implement any reasonable UVC recommendations. If Client fails to do so, this SLA will not apply.

5.5 Governance and Escalation

UVC and Client will hold regular meetings to review and assess Service Level Performance, address any Client concerns, and work in good faith to resolve any disputes between the Parties with respect to Service Level Performance.

5.6 Service Levels

UVC services include Service Levels. The following criteria have associated service levels assigned to Portal Availability.

Portal Availability
Definitions: "Availability" means the following, converted to a percentage: **Calculation:** (Number of minutes in the month – Outage Time) / Number of minutes in the month. **Portal Availability:** The availability of the web accessible portal made available to Customer to view reports and submit tickets. Outage Time shall commence upon the earlier of: (1) UVC's detecting the outage and logging an Incident ticket or (2) UVC's logging an Incident ticket upon Customer's notice to UVC of the outage, which notice contains sufficient information to confirm that the outage is occurring in the System. The Outage Time ends when the System is returned to a usable level of service. The duration of Outage time shall be rounded to the nearest minute. UVC will log an Incident ticket promptly following notification from Customer or its own detection of an outage.
Service Level Platform Availability: 99.9% Portal Availability: 99%
Measurement Period: Monthly (one calendar month)

Containment Service Level Description	Service Level Target	Client Requirements
Definition: P1 – Critical Priority Issue: In the event of a P1 Issue (defined as an issue that prevents Client from accessing the Service), UVC will respond as follows	99%	Client will provide information about impact and threat

• Initial Response: < 8 hours • Status Update: 24 hours		
Definition: P2 – High Priority Issue: In the event of a P2 Issue (defined as an issue in which Client can access the Service, however, one or more significant functions are unavailable, such as the ability to launch a scan or map), UVC will respond as follows: • Initial Response: < 24 hours • Status Update: 2 business days	99%	Client will provide information about impact and threat

“Initial Response” is defined as the initial contact from UVC following the creation and submission of a P1 or P2 related ticket by Client or UVC.

A status update will be communicated to Client if the incident cannot be resolved immediately. A final follow-up with Client occurs on the resolution date. The issue will remain open until the issue is resolved, in UVC’ reasonable opinion.